



AFRL Defensive IO Programs

William E Wolf
AFRL/IFGB
525 Brooks Road
Rome NY 13441
wolfw@rl.af.mil

Lt Col Richard Simpson
AFRL/HEX
2255 H St. Bldg 248
WPAF Ohio 45433
Richard.Simpson@wpafb.af.mil

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 22-04-2002		2. REPORT TYPE Briefing		3. DATES COVERED (FROM - TO) xx-xx-2002 to xx-xx-2002	
4. TITLE AND SUBTITLE AFRL Defensive IO Programs Unclassified				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Wolf, William E. ; Simpson, Richard ;				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME AND ADDRESS AFRL/IFGB 525 Brooks Road Rome, NY13441				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS USAF ,				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT APUBLIC RELEASE ,					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT See report.					
15. SUBJECT TERMS IATAC Collection					
16. SECURITY CLASSIFICATION OF:		17. LIMITATION OF ABSTRACT Public Release	18. NUMBER OF PAGES 17	19. NAME OF RESPONSIBLE PERSON Email from Booz, Allen, & Hamilton (IATAC), (blank) lfenster@dtic.mil	
a. REPORT Unclassified	b. ABSTRACT Unclassified			c. THIS PAGE Unclassified	19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007
				Standard Form 298 (Rev. 8-98) Prescribed by ANSI Std Z39.18	

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 074-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 4/22/2002	3. REPORT TYPE AND DATES COVERED Briefing 4/22/2002	
4. TITLE AND SUBTITLE AFRL Defensive IO Programs			5. FUNDING NUMBERS	
6. AUTHOR(S) Wolf, William E.; Simpson, Lt. Col Richard				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Air Force Research Laboratory 525 Brooks Rd. Rome, NY 13441			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Air Force Research Laboratory 525 Brooks Road, Rome NY 13441			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; Distribution unlimited			12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 Words) This briefing on Defense IO Programs was presented during the Phoenix Challenge 2002 Conference & Warfighter Day.				
14. SUBJECT TERMS IATAC Collection, information operations, Cyber Wolf			15. NUMBER OF PAGES 16	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UNLIMITED	



Information Assurance



- **Definition**

- Information operations that defend the global information enterprise through employment of **Protect, Detect, Assess and Respond** capabilities. This is accomplished by ensuring availability, integrity, authentication, confidentiality, and non-repudiation (based on DODD S-3600.1 & AFDD 2-5).

- **Approach**

- Develop technology for and transition technology to AF, DoD and National customers
- Continuous capability improvement through experimentation with warfighter, spiral development, leverage of COTS, and technology transition, e.g., CAOC-X, JBI, etc...

- **Value to the Warfighter**

- Accurate, trusted, reliable warfighter information
- Survivable information systems and networks
- Information superiority through assured information operations



Information Assurance

“A Short History”



- **Pre 1970's**
 - Encryption
- **1970's**
 - Computer Security R&D begins (“Test and Patch”)
- **1980's**
 - Multilevel Security
 - Strong Security Based on Special-Purpose Systems
 - Risk Avoidance
 - “Orange Book” Evaluation Criteria
- **1990's**
 - Movement Towards COTS Software
 - Perfect Security Recognized as Unachievable
 - Risk Management
- **2000 & Beyond**
 - Trend toward Information Survivability
 - Situational Awareness
 - Intrusion Tolerance
 - Active Response



Information Assurance Today's Capability



Protect

- Encryption (VPN, Digital Signature, PKI, etc.)
- Firewalls/Guards/Boundary Controllers
- Passwords, Biometrics
- Trusted Operating Systems/Database Management Systems
- Physical Security (Stovepipes, Vaults, etc.)
- Vulnerability Scanners
- “Penetrate and Patch”

Detect

- Virus Scanners (Signature-Based)
- Intrusion-Detection (Signature-Based)
- Auditing

Assess

- Computer Forensics Tools (Media Imaging, Data Recovery, etc.)
- CERT's

Respond

- Physical Media Relocation
- Backups



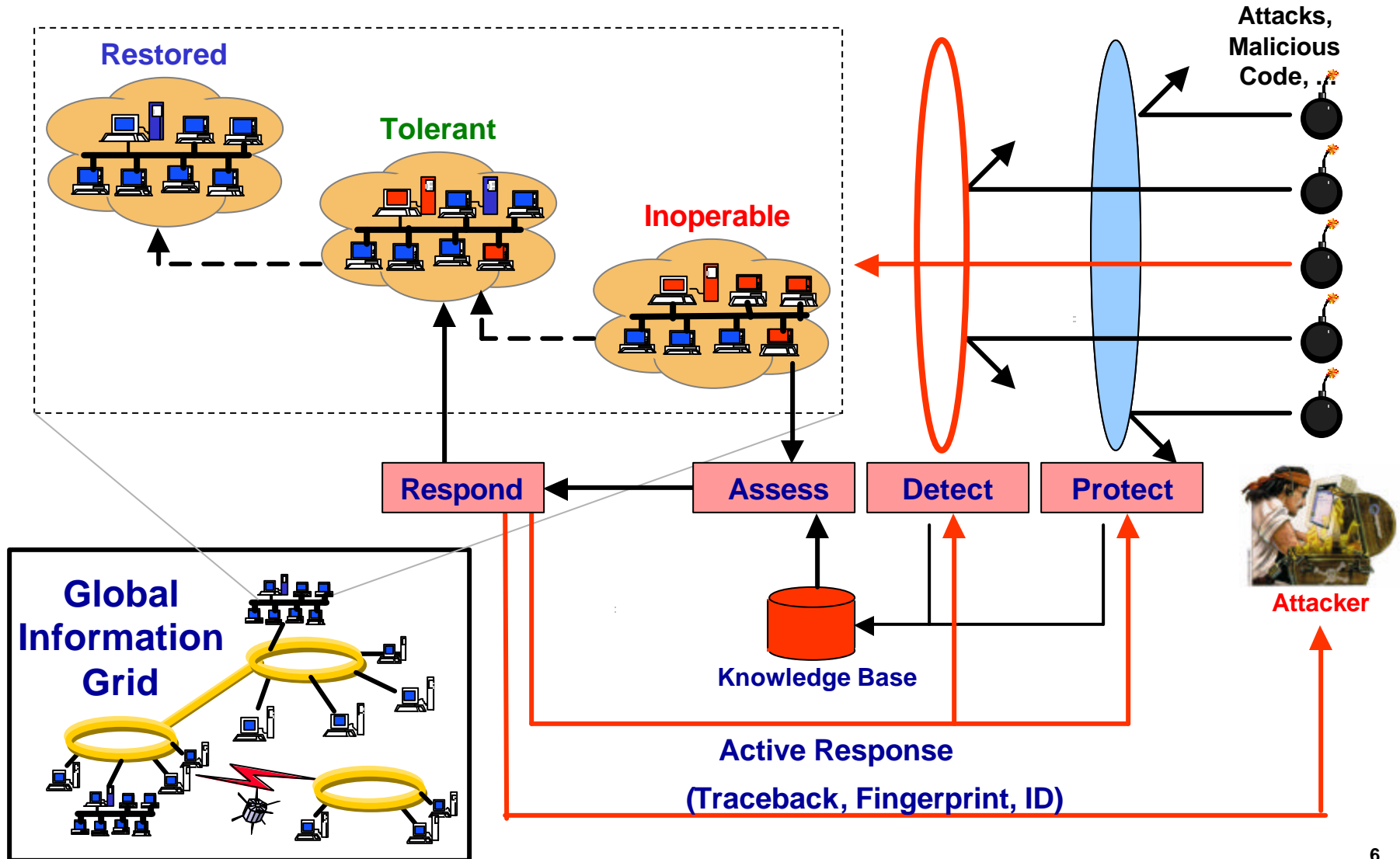
Vision



- **Protect the GIE with a high degree of confidence**
 - Assured defense-in-depth against a wide variety of threats
 - Understand/manage risks and plan for protection
- **Detect information attacks**
 - Early warning using light weight cooperating sensors
 - Efficient, accurate data reduction, fusion, correlation
- **Assess information attacks**
 - Identify adversary, nature, timing, severity
 - Determine mission impact
 - Develop courses-of-action
- **Respond to a successful IW attack in an appropriate manner**
 - Graceful degradation, recovery, reconstitution
 - Feedback to improve protection and detection processes
 - Offensive Information Operations



Information Assurance Vision





National Scale INFOSEC Hard Problems

[By the INFOSEC Research Council]



- **Intrusion/Misuse Detection & Response**
- **Foreign & Mobile Code**
- **Controlled Sharing of Sensitive Information**
- **Application Security**
- **Denial-of-Service**
- **Communications Security**
- **Security Management Infrastructure**
- **Security in Mobile Environments**
- **Security Engineering Methodologies**
- **Influencing Vendors**



Technical Approach



High Assurance

RF Protect

Secure Mobile Code

Boundary Controllers

Embedded Systems IA

Wrappers

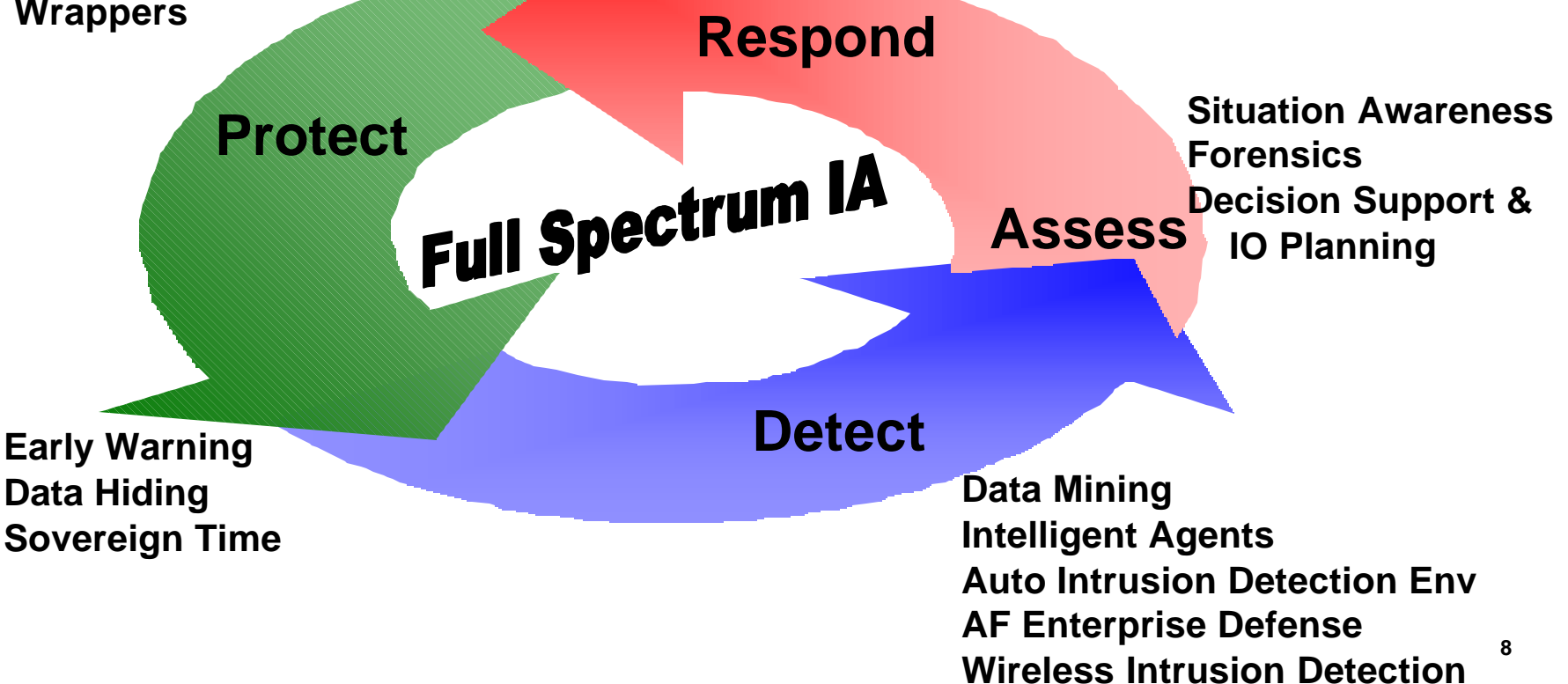
Intrusion Tolerance

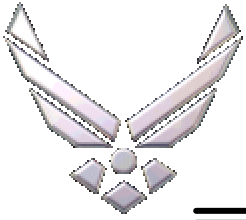
Active Response

Fault Tolerant Networks

Effects-Based IO

Assured QoS





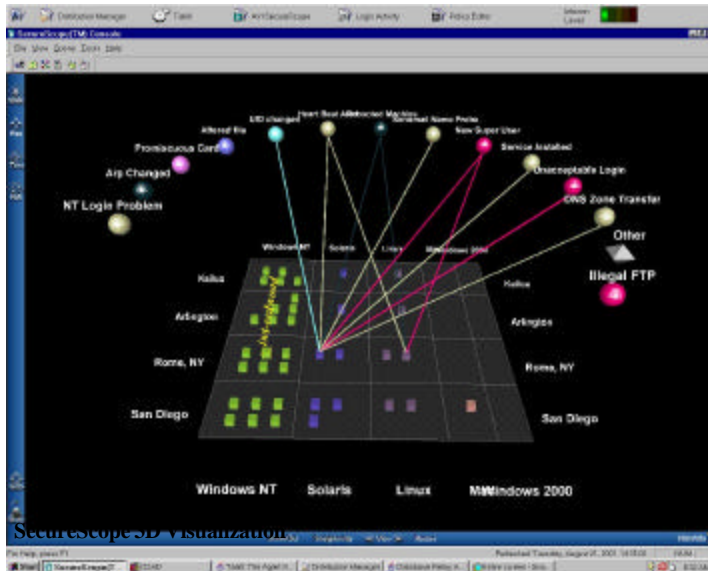
Success Stories



- **DAIWatch**
- **CYBERWOLF**
- **Wireless Information Assurance**
- **Steganography**
- **Air Force Enterprise Defense (AFED)**



Distributed Agents for Information Warfare Operational Transition (DAIWatch)



Objective: Enhance level of Information Assurance by utilizing breakthroughs in software agent and fusion technologies that provide revolutionary flexibility, extensibility, and reliability

Approach:

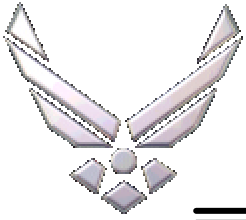
- Agent Technology via Java Aglets
- Dynamic distribution of multiple host sensors
- Integrated multi-dimension graphical analysis

DAIWatch Revolution

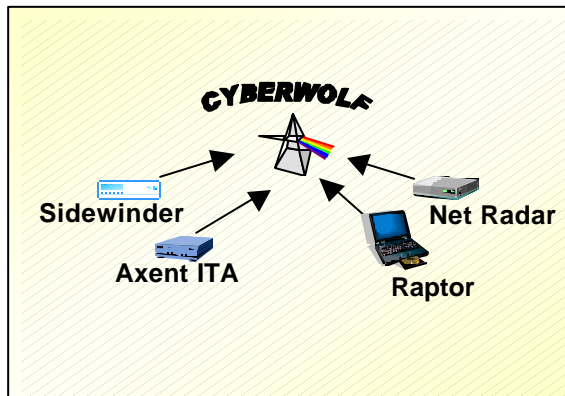
- Finds the most sophisticated attackers
- Reduces security administration
- Adjusts to risk and minimizes overhead
- Not vulnerable to compromise

Technology Transition

- Phase III SBIR
- AFIWC – agreements to integrate DAIWatch with CIDDS
- JBC – DAIWatch selected for operational demonstration (focused on ability to transport functions and data across SIPRnet)
- Beta Test Program with a commercial investment company



CYBERWOLF



Status

- Cyberwolf correlating events from AFRL RRS NOC
- Cyberwolf commercialization effort fully underway with several potential customers
- Correlation capability from Cyberwolf is being channeled into AFED program
- Rule set currently exceeding 2000 entries
- Cyberwolf under evaluation for use by several large corp. and a Canadian bank for network enterprise protection

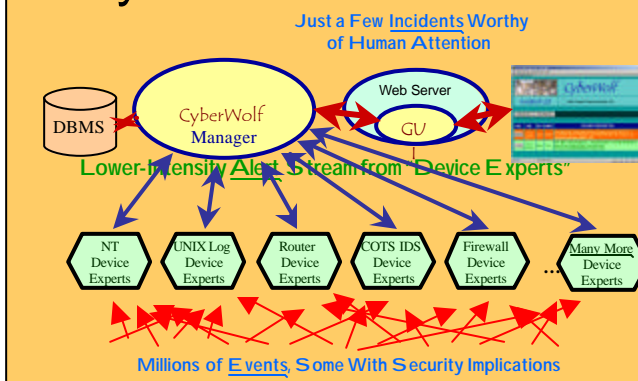
Problem: Network Defenders cannot process thousands of low level events in real time.

Objective: Enhance network defense by automatically correlating network management events with Intrusion Detection System (IDS) events to provide accurate situational information

Approach:

- Place lightweight device experts on all network assets
- Device experts adaptable to specific installations operational security policy
- Remotely manage geographically separate installations in a 24/7 mode

CyberWolf Architecture



Technical Challenges

- Distribute event processing between enterprise and device
- Design and implement device experts for all types of network assets
- Encapsulate Net defenders knowledge into Rule structure
- Reduce 1000's of net events to a few highly reliable incidents

Tech Transitions

Federal Emergency Management Agency
Naval Sea Systems Command
Air Force Research Lab
Joint Battle Center
Land Information Warfare Activity

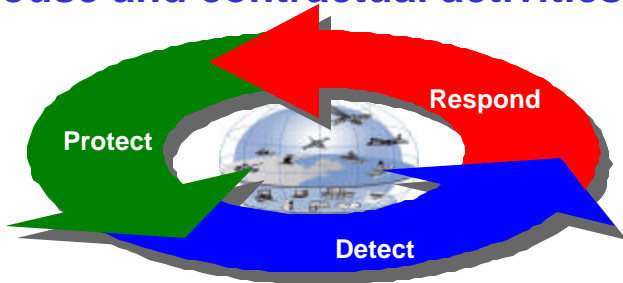




AFRL Wireless IA Program



Objective: *Enhance and extend IA for wireless through synergistic in-house and contractual activities*



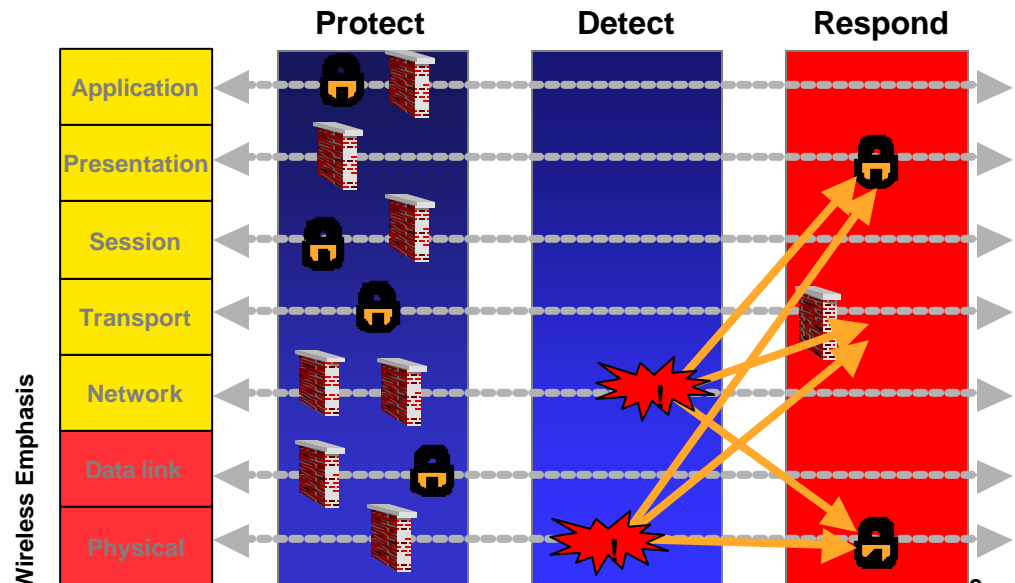
Current Projects:

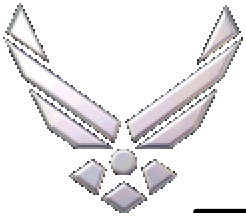
- Wireless Intrusion Detection & Distributed Boundary Control
- Combined Access Point/Firewall/VPN/Intrusion Sensor Device
- Wireless & Mobile Authentication/Key Revocation
- Adaptive RF Wireless Nodes
- Software Defined Radio for Wireless Information Assurance
- Intrusion Detection Agents for Handheld Devices
- Automated Wireless LAN Compliance Monitoring Techniques
- AF Wireless Security Architecture Development
- DOD Overarching Wireless Policy Development

Accomplishments:

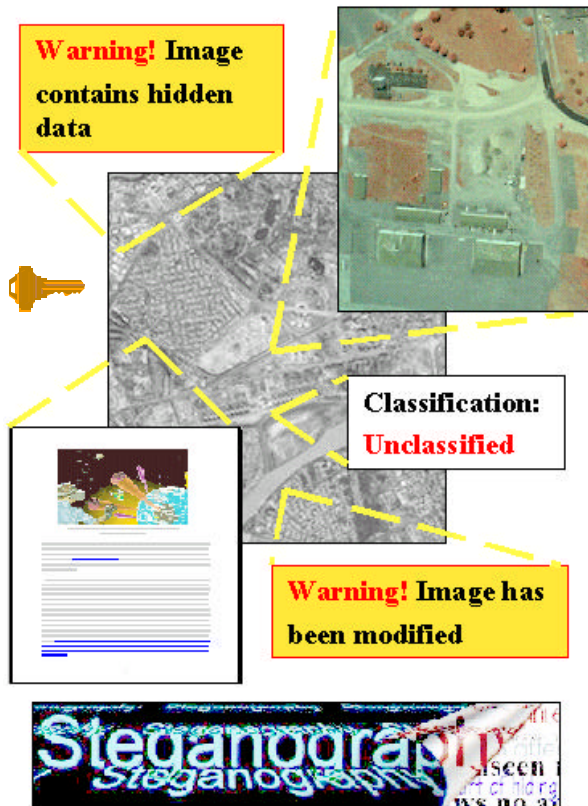
- Developed site survey and compliance monitoring techniques
- Created wireless architecture adopted by AF
- Developed and demonstrated wireless intrusion detection and policy violation detection techniques
- Provided key inputs to DOD overarching policy
- Assessed netstumbler.com threat in the context of AF base locations

Wireless IA Problem Space:





Smart Digital Data

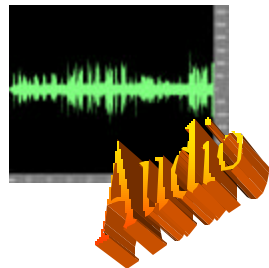


Data Hiding/Embedding

Steganography

Watermarking

Steganalysis

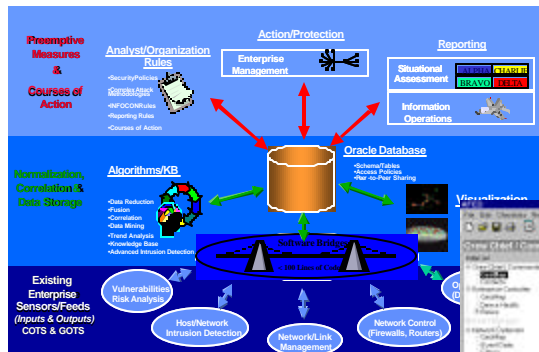


Technology Area Payoff

- Information Assurance
 - data & source authentication
 - tamper detection & data recovery
 - automatic data dissemination through guards; classification & license marking
 - detection & identification of adversary steganographic activity & extraction of hidden data
 - tracing sources of data leaks
 - minimize data loss (corrupt data pointers; invalid data headers)
- Information Enhancement
 - embedded auxiliary information (images, documents, overlays, audio, links, etc.)
 - multi-level data release to coalition forces; key-based access
 - covert communication
 - maximize throughput of communication channels

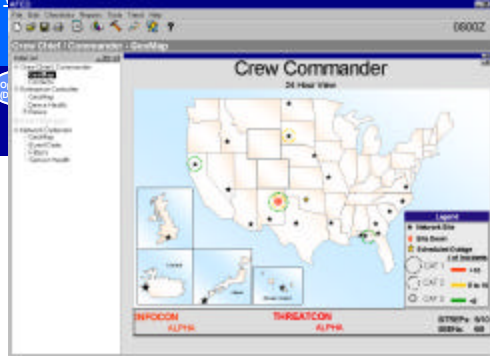


Air Force Enterprise Defense (AFED)



Infrastructure

Interface



Objectives

- Provide a **Defense-in-Depth** capability that integrates existing event information:
 - Policy Enforcement; Change/Configuration Management; Threat & Vulnerability Assessment with Countermeasure recommendations; Intrusion Detection; Network Management
- **Fuse** Information Assurance (IA) and Network Management data into a **Common Enterprise Picture**
- Provide a **consistent visual environment** for information portrayal

Approach

- Spiral tech exploration, development, validation, and feedback process
 - Automated Reporting for Containment and IO Targeting
 - Mission Situational Assessment
 - Automated Courses of Action

Transition Agents: ESC/DIGC, ESC/DIW
End Users: MAJCOM NOSCs, AFNOSC, CAOC-x

Payoffs

- **Integrates existing enterprise sensors** and provides enhanced Information Assurance and Enterprise Defense capabilities in support of the AF Protect-Detect-React/Restore model.
- Assists in the **automated detection and reporting** of information attacks, containment and restoration of compromised systems, and planning/protection of enterprise assets.
- Supports entire NOSC mission by **cross-sharing of data** among NOSC crew

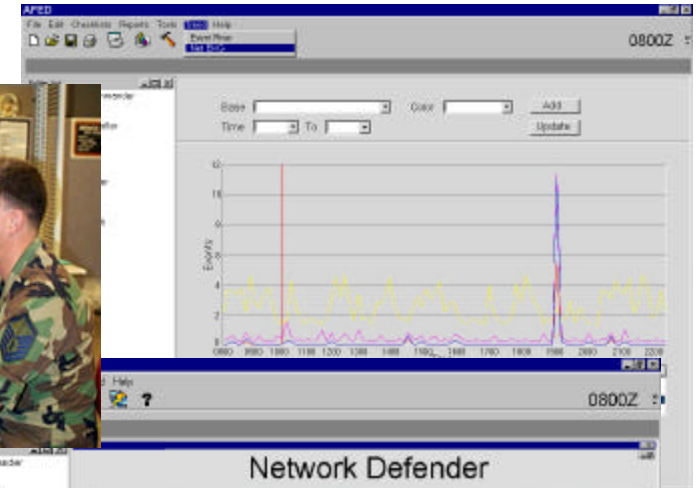
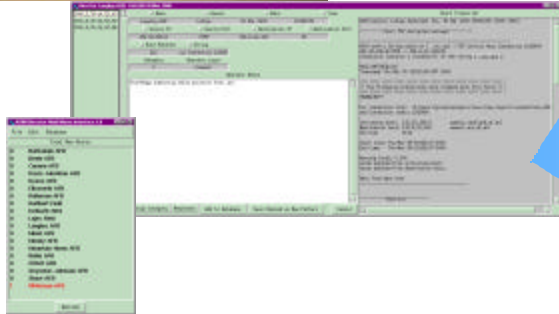


Air Force Enterprise Defense

Moving from Data-Centric to Mission-Centric Operations

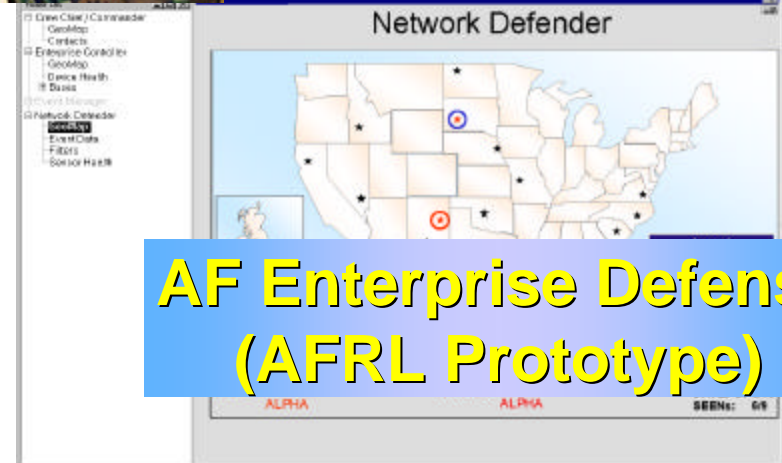


**State of the Practice
(NOSC Interface)**



Vision

- “NOSC-in-a-box”—one application integrates all NOSC tools
- One application addresses needs of entire NOSC crew



**AF Enterprise Defense
(AFRL Prototype)**



Summary



- **The AFRL/IF program includes all aspects of the IA problem**
 - Protect
 - Detect
 - Assess
 - Respond
- **Addressing the hard IA problems**
 - Leading edge technology
- **Addressing technology at all levels**
 - Basic Research
 - Exploratory Development
 - Advanced Development

